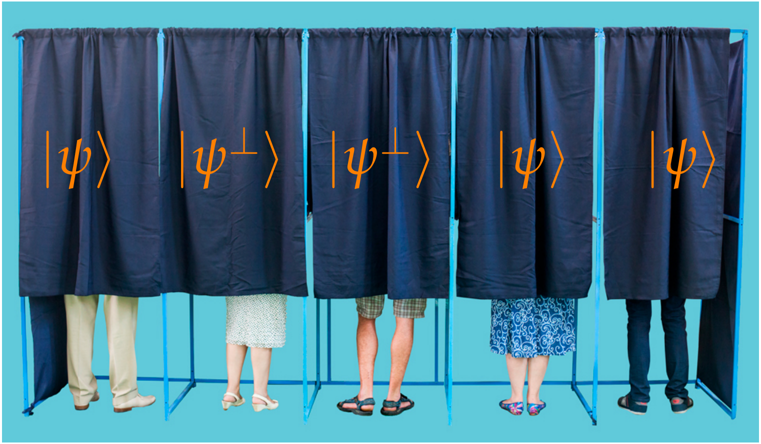
Quantum majority

and other Boolean functions with quantum inputs



Harry Buhrman

Laura Mančinska

Māris Ozols

Noah Linden

Ashley Montanaro

Manifesto

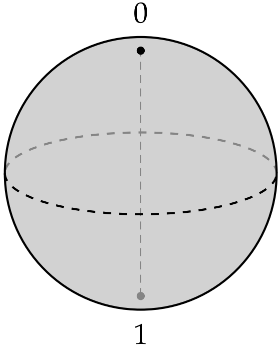
- All information is quantum…

Manifesto

- All information is quantum…
- …there is no classical information

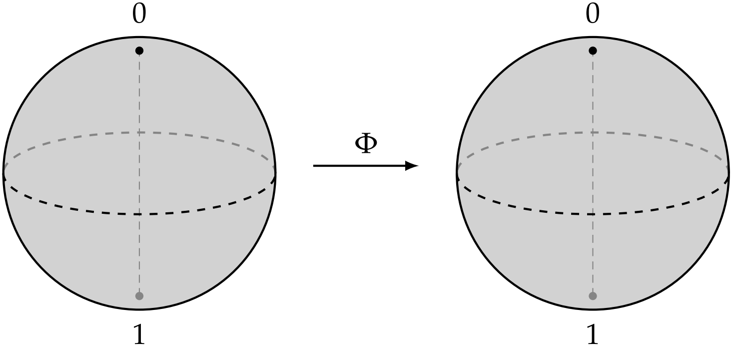
Manifesto

- All information is quantum…
- …there is no classical information



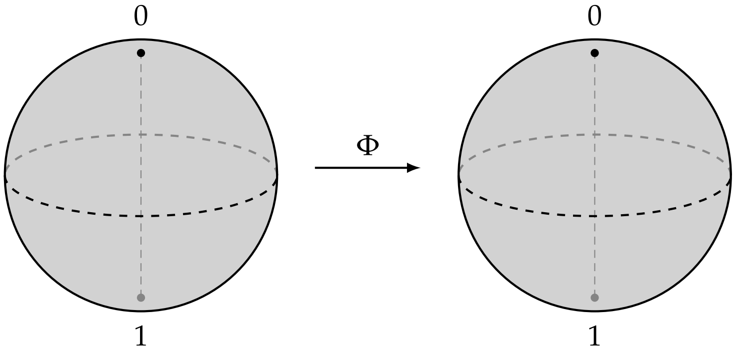
Manifesto

- All information is quantum…
- …there is no classical information
- Algorithm = CPTP map

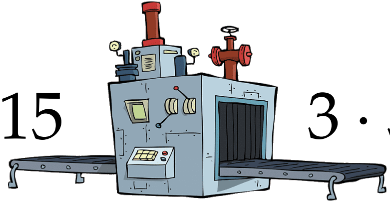


Manifesto

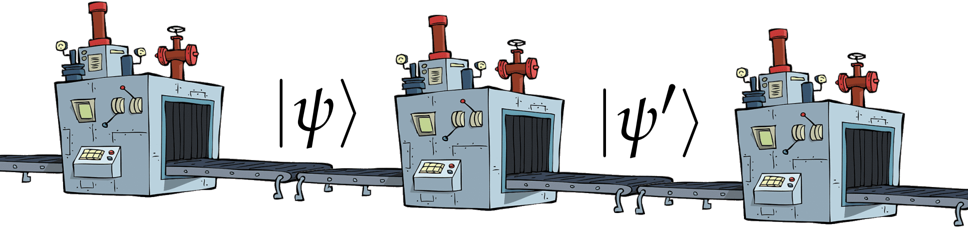
- All information is quantum…
- …there is no classical information
- Algorithm = CPTP map
- Classical computer science is dead!



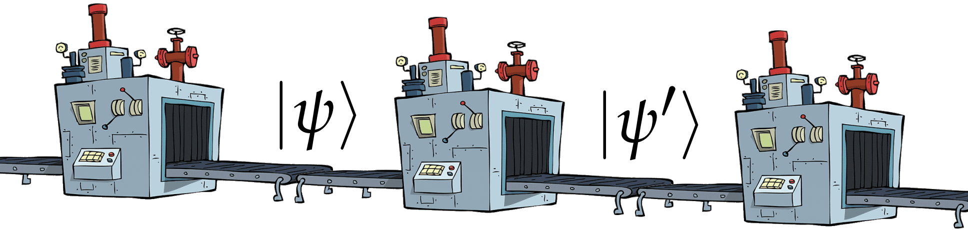
Manifesto (lite)

15  $3 \cdot 5$

Manifesto (lite)



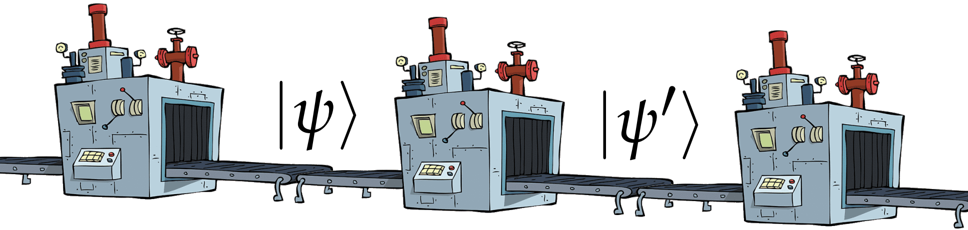
Manifesto (lite)



- quantum Fourier transform
- Grover iteration
- swap test
- …

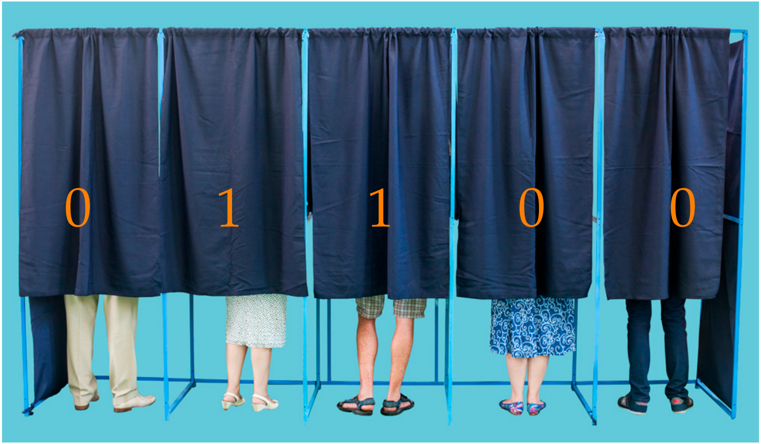
Manifesto (lite)

New *quantum* primitives!

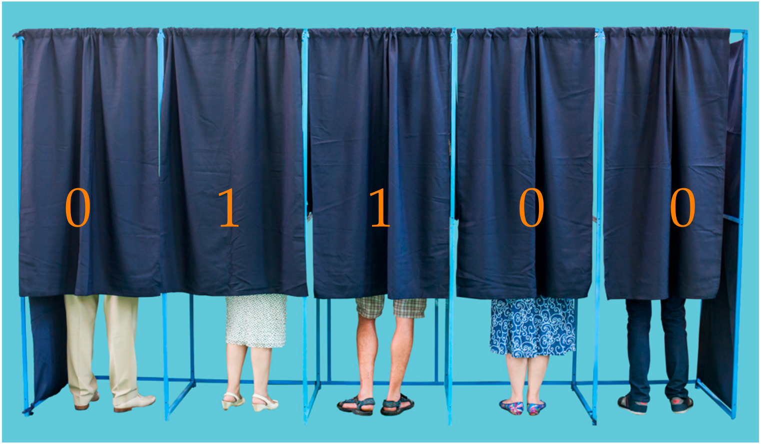


- quantum Fourier transform
- Grover iteration
- swap test
- …

Majority vote

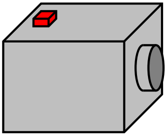


Majority vote

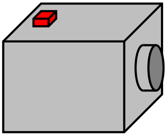


- success amplification
- error correction
- democracy

Quantum majority vote

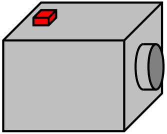


Quantum majority vote



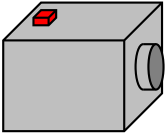
$|\psi\rangle$

Quantum majority vote



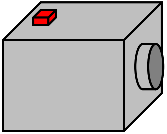
$|\psi\rangle|\psi\rangle$

Quantum majority vote



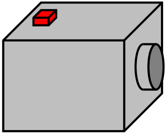
$|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle$

Quantum majority vote



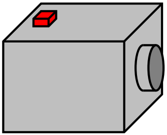
$$|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle$$

Quantum majority vote



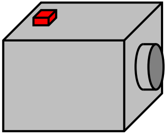
$$|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle$$

Quantum majority vote



$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

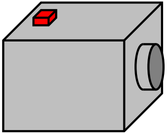
Quantum majority vote



$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

Computation in an unknown basis

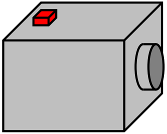
Quantum majority vote



$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

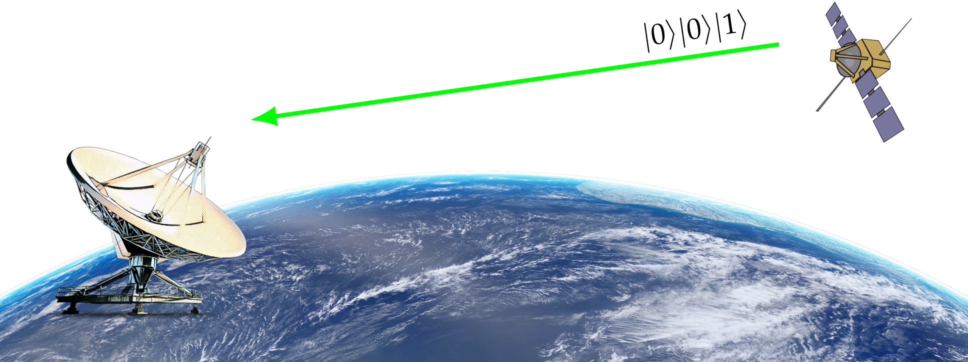
Computation in an unknown basis

Quantum majority vote

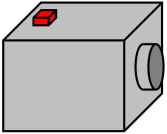


$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

Computation in an unknown basis

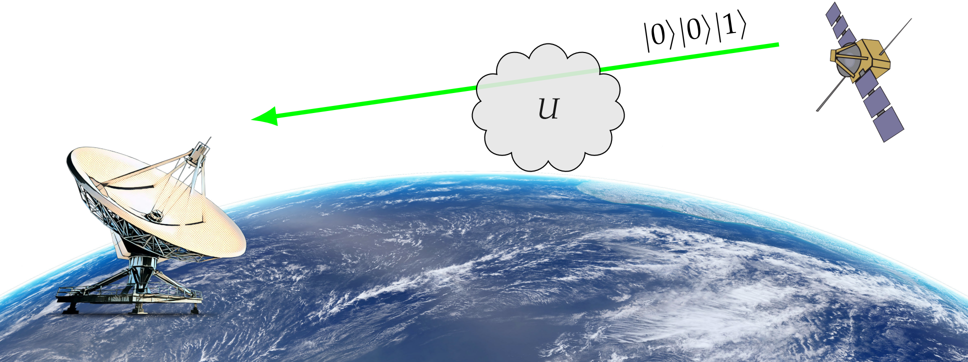


Quantum majority vote

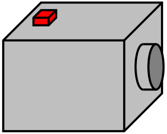


$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

Computation in an unknown basis

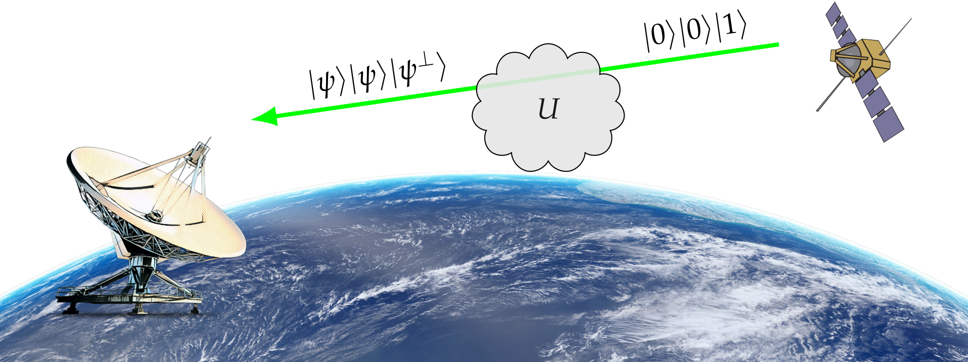


Quantum majority vote

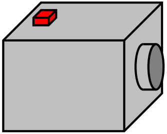


$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

Computation in an unknown basis

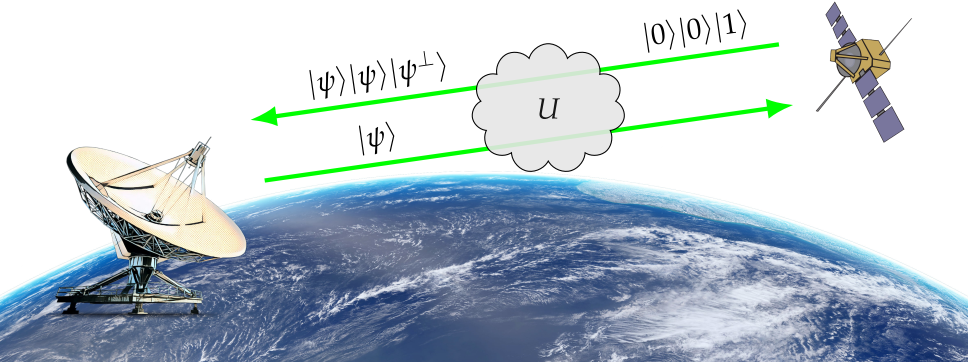


Quantum majority vote

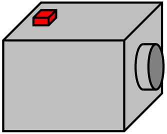


$$\underbrace{|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi^{\perp}\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

Computation in an unknown basis

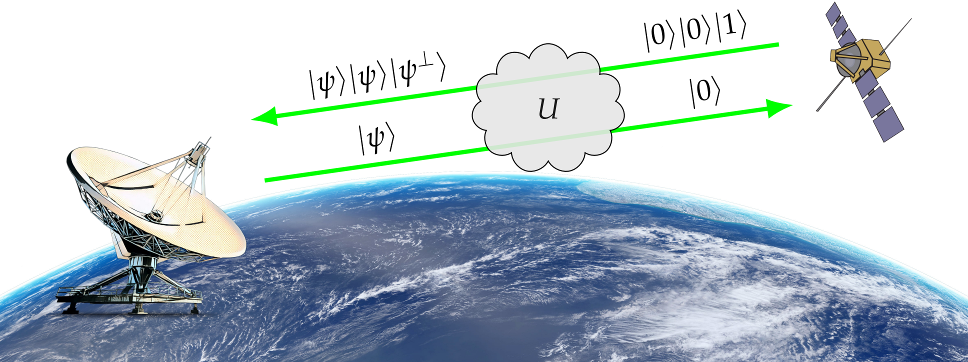


Quantum majority vote



$$\underbrace{|\psi\rangle|\psi\rangle|\psi^\perp\rangle|\psi\rangle|\psi\rangle|\psi^\perp\rangle|\psi\rangle|\psi\rangle|\psi\rangle}_{|\psi\rangle}$$

Computation in an unknown basis



Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$|x\rangle \mapsto \quad |f(x)\rangle \qquad \forall x \in \{0,1\}^n$$

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

XOR of two bits

$$|0\rangle \otimes |1\rangle \mapsto |1\rangle$$

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

XOR of two bits

$$|0\rangle \otimes |1\rangle \mapsto |1\rangle$$

$$U|0\rangle \otimes U|1\rangle \mapsto U|1\rangle$$

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

XOR of two bits

$$|0\rangle \otimes |1\rangle \mapsto |1\rangle$$

$$X|0\rangle \otimes X|1\rangle \mapsto X|1\rangle$$

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

XOR of two bits

$$|0\rangle \otimes |1\rangle \mapsto |1\rangle$$

$$X|0\rangle \otimes X|1\rangle \mapsto X|1\rangle$$

$$|1\rangle \otimes |0\rangle \mapsto |0\rangle$$

Windows

An error has occurred. To continue:

Press Enter to return to Windows, or

Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.

Error: 0E : 016F : BFF9B3D4

Press any key to continue _

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

XOR of two bits

$$|0\rangle \otimes |1\rangle \mapsto |1\rangle$$

$$X|0\rangle \otimes X|1\rangle \mapsto X|1\rangle$$

$$|1\rangle \otimes |0\rangle \mapsto |0\rangle$$

Covariance

Unitary covariance

Computing $f : \{0,1\}^n \to \{0,1\}$ in a *unitary-covariant* way:

$$U^{\otimes n}|x\rangle \mapsto U|f(x)\rangle \qquad \forall x \in \{0,1\}^n, U \in \mathrm{U}(2)$$

XOR of two bits

$$|0\rangle \otimes |1\rangle \mapsto |1\rangle$$

$$X|0\rangle \otimes X|1\rangle \mapsto X|1\rangle$$

$$|1\rangle \otimes |0\rangle \mapsto |0\rangle$$

Covariant functions

$f : \{0,1\}^n \to \{0,1\}$ is *covariant* (or *self-dual*) if

$$f(\overline{x}) = \overline{f(x)}$$

Symmetric functions

Assumption

$f(x)$ depends only on the Hamming weight of $x \in \{0, 1\}^n$

Symmetric functions

Assumption

$f(x)$ depends only on the Hamming weight of $x \in \{0,1\}^n$

Example: $n = 3$

$\lvert x \rvert$	0	1	2	3
$f(x)$	0	0	1	1

Symmetric functions

Assumption

$f(x)$ depends only on the Hamming weight of $x \in \{0,1\}^n$

Example: $n = 3$

$\lvert x \rvert$	0	1	2	3
$f(x)$	0	0	1	1

Even n is bad

$$f(0,1) = \overline{f(1,0)} = \overline{f(0,1)}$$

Problem

Assumptions

Given $f : \{0,1\}^n \to \{0,1\}$, assume

- f is covariant
- f is symmetric
- n is odd

Problem

Assumptions

Given $f : \{0,1\}^n \to \{0,1\}$, assume

- f is covariant
- f is symmetric
- n is odd

Goal

Given $U^{\otimes n}|x\rangle$, for an unknown $U \in \mathrm{U}(2)$ and $x \in \{0,1\}^n$, produce ρ that is close to $U|f(x)\rangle$.

Problem

Assumptions

Given $f : \{0,1\}^n \to \{0,1\}$, assume

- f is covariant
- f is symmetric
- n is odd

Goal

Given $U^{\otimes n}|x\rangle$, for an unknown $U \in \mathrm{U}(2)$ and $x \in \{0,1\}^n$, produce ρ that is close to $U|f(x)\rangle$.

Worst-case fidelity

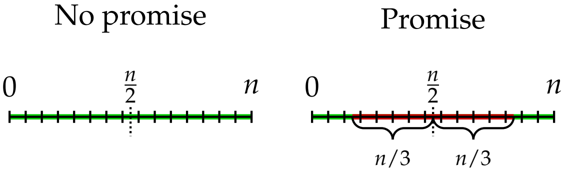
$$F_f := \max_{\Phi} \min_{x,U} \langle f(x)|U^\dagger \, \Phi\Big(U^{\otimes n}|x\rangle\langle x|U^{\dagger\otimes n}\Big) \, U|f(x)\rangle$$

Results on majority

Trivial strategy: Output any qubit at random

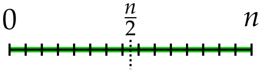
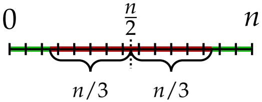
Results on majority

Trivial strategy: Output any qubit at random



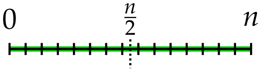
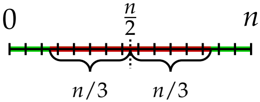
Results on majority

Trivial strategy: Output any qubit at random

	No promise	Promise
		
Trivial	$\frac{1}{2}+\frac{1}{2n}$	$\frac{5}{6}$

Results on majority

Trivial strategy: Output any qubit at random

	No promise 	Promise 
Trivial	$\frac{1}{2} + \frac{1}{2n}$	$\frac{5}{6}$
Optimal	$\frac{1}{2} + \Theta\left(\frac{1}{\sqrt{n}}\right)$	$1 - \Theta\left(\frac{1}{n}\right)$

Symmetric / anti-symmetric subspace of $\mathbb{C}^2 \otimes \mathbb{C}^2$

Symmetric states:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} |00\rangle = \begin{pmatrix} a^2 \\ ac \\ ca \\ c^2 \end{pmatrix} = a^2 \; |00\rangle \; + \sqrt{2}ac \; \frac{|01\rangle + |10\rangle}{\sqrt{2}} \; + c^2 \; |11\rangle$$

Symmetric / anti-symmetric subspace of $\mathbb{C}^2 \otimes \mathbb{C}^2$

Symmetric states:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} |00\rangle = \begin{pmatrix} a^2 \\ ac \\ ca \\ c^2 \end{pmatrix} = a^2 \underbrace{|00\rangle}_{0} + \sqrt{2}ac \underbrace{\frac{|01\rangle + |10\rangle}{\sqrt{2}}}_{1} + c^2 \underbrace{|11\rangle}_{2}$$

Symmetric / anti-symmetric subspace of $\mathbb{C}^2 \otimes \mathbb{C}^2$

Symmetric states:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} |00\rangle = \begin{pmatrix} a^2 \\ ac \\ ca \\ c^2 \end{pmatrix} = a^2 \underbrace{\boxed{|00\rangle}}_{0} + \sqrt{2}ac \underbrace{\boxed{\frac{|01\rangle + |10\rangle}{\sqrt{2}}}}_{1} + c^2 \underbrace{\boxed{|11\rangle}}_{2}$$

Anti-symmetric state (singlet):

$$|\Psi^-\rangle := \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Symmetric / anti-symmetric subspace of $\mathbb{C}^2 \otimes \mathbb{C}^2$

Symmetric states:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} |00\rangle = \begin{pmatrix} a^2 \\ ac \\ ca \\ c^2 \end{pmatrix} = a^2 \underbrace{\boxed{|00\rangle}}_{0} + \sqrt{2}ac \underbrace{\boxed{\frac{|01\rangle + |10\rangle}{\sqrt{2}}}}_{1} + c^2 \underbrace{\boxed{|11\rangle}}_{2}$$

Anti-symmetric state (singlet):

$$|\Psi^-\rangle := \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} |\Psi^-\rangle = (ad - bc)|\Psi^-\rangle$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\mathrm{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\mathrm{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

Schur transform on two qubits

$$U_{\text{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\text{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\text{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

Schur transform on two qubits

$$U_{\text{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\text{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\text{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\mathrm{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\mathrm{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

$$U_{\mathrm{Sch}}\, \mathrm{SWAP}\, U_{\mathrm{Sch}}^{\dagger} = \mathrm{diag}(-1, 1, 1, 1)$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\mathrm{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\mathrm{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

$$U_{\mathrm{Sch}}\, \mathrm{SWAP}\, U_{\mathrm{Sch}}^{\dagger} = \mathrm{diag}(-1, 1, 1, 1)$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\mathrm{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\mathrm{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

$$U_{\mathrm{Sch}}\, \mathrm{SWAP}\, U_{\mathrm{Sch}}^{\dagger} = \mathrm{diag}(-1, 1, 1, 1)$$

Schur transform on two qubits

$$U_{\mathrm{Sch}} := \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$U_{\mathrm{Sch}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\otimes 2} U_{\mathrm{Sch}}^{\dagger} = \begin{pmatrix} ad - bc & 0 & 0 & 0 \\ 0 & a^2 & \sqrt{2}ab & b^2 \\ 0 & \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ 0 & c^2 & \sqrt{2}cd & d^2 \end{pmatrix}$$

$$U_{\mathrm{Sch}}\,\mathrm{SWAP}\,U_{\mathrm{Sch}}^{\dagger} = \mathrm{diag}(-1,1,1,1)$$

Each block defines a homomorphism: $Q(MN) = Q(M)Q(N)$

Schur transform on n qubits

$$U_{\mathrm{Sch}} : (\mathbb{C}^2)^{\otimes n} \to \bigoplus_{\lambda \vdash n} \left[\mathbb{C}^{m_\lambda} \otimes \mathbb{C}^{d_\lambda} \right]$$

Schur transform on n qubits

$$U_{\mathrm{Sch}} : (\mathbb{C}^2)^{\otimes n} \to \bigoplus_{\lambda \vdash n} \left[\mathbb{C}^{m_\lambda} \otimes \mathbb{C}^{d_\lambda} \right]$$

$$U_{\mathrm{Sch}} M^{\otimes n} U_{\mathrm{Sch}}^\dagger = \bigoplus_{\lambda \vdash n} \left[Q_\lambda(M) \otimes I_{d_\lambda} \right]$$

Schur transform on n qubits

$$U_{\mathrm{Sch}} : (\mathbb{C}^2)^{\otimes n} \to \bigoplus_{\lambda \vdash n} \left[\mathbb{C}^{m_\lambda} \otimes \mathbb{C}^{d_\lambda} \right]$$

$$U_{\mathrm{Sch}} M^{\otimes n} U_{\mathrm{Sch}}^\dagger = \bigoplus_{\lambda \vdash n} \left[Q_\lambda(M) \otimes I_{d_\lambda} \right]$$

$$U_{\mathrm{Sch}} \pi U_{\mathrm{Sch}}^\dagger = \bigoplus_{\lambda \vdash n} [I_{m_\lambda} \otimes P_\lambda(\pi)]$$

Schur transform on n qubits

$$U_{\mathrm{Sch}} : (\mathbb{C}^2)^{\otimes n} \to \bigoplus_{\lambda \vdash n} \left[\mathbb{C}^{m_\lambda} \otimes \mathbb{C}^{d_\lambda} \right]$$

$$U_{\mathrm{Sch}} M^{\otimes n} U_{\mathrm{Sch}}^\dagger = \bigoplus_{\lambda \vdash n} \left[Q_\lambda(M) \otimes I_{d_\lambda} \right]$$

$$U_{\mathrm{Sch}} \pi U_{\mathrm{Sch}}^\dagger = \bigoplus_{\lambda \vdash n} \left[I_{m_\lambda} \otimes P_\lambda(\pi) \right]$$

Can be implemented with $O(n^4 \log n)$ gates
(Kirby & Strauch, 2017)

Algorithm

Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}

Algorithm

Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}
2. Measure $\lambda \vdash n$ (*weak Schur sampling*)

Algorithm

Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}
2. Measure $\lambda \vdash n$ (*weak Schur sampling*)
3. Discard the permutation register

Algorithm

Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}
2. Measure $\lambda \vdash n$ (*weak Schur sampling*)
3. Discard the permutation register
4. Apply some covariant channel with 1-qubit output

Algorithm

Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}
2. Measure $\lambda \vdash n$ (*weak Schur sampling*)
3. Discard the permutation register
4. Apply some covariant channel with 1-qubit output

- Steps 1–3 are reversible (generic pre-processing)

Algorithm

Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}
2. Measure $\lambda \vdash n$ (*weak Schur sampling*)
3. Discard the permutation register
4. Apply some covariant channel with 1-qubit output

- Steps 1–3 are reversible (generic pre-processing)
- Step 4 acts on a state of random dimension m_λ

Algorithm

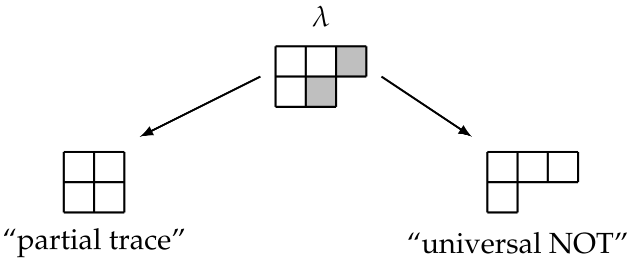
Input: $U^{\otimes n}|x\rangle$ with unknown $x \in \{0,1\}^n$ and $U \in \mathrm{U}(2)$

1. Apply Schur transform U_{Sch}
2. Measure $\lambda \vdash n$ (*weak Schur sampling*)
3. Discard the permutation register
4. Apply some covariant channel with 1-qubit output

- Steps 1–3 are reversible (generic pre-processing)
- Step 4 acts on a state of random dimension m_λ
- Only step 4 depends on f

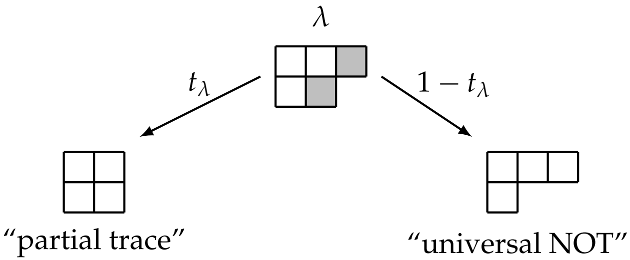
Extremal covariant channels

For each $\lambda \vdash n$, only two *extremal* covariant channels from $\mathbb{C}^{m_\lambda} \to \mathbb{C}^2$:



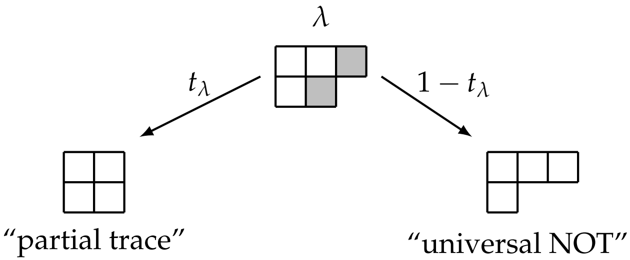
Extremal covariant channels

For each $\lambda \vdash n$, only two *extremal* covariant channels from $\mathbb{C}^{m_\lambda} \to \mathbb{C}^2$:



Extremal covariant channels

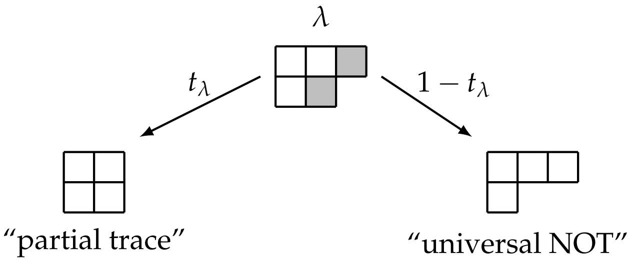
For each $\lambda \vdash n$, only two *extremal* covariant channels from $\mathbb{C}^{m_\lambda} \to \mathbb{C}^2$:



- A "dual" Clebsch–Gordan transform

Extremal covariant channels

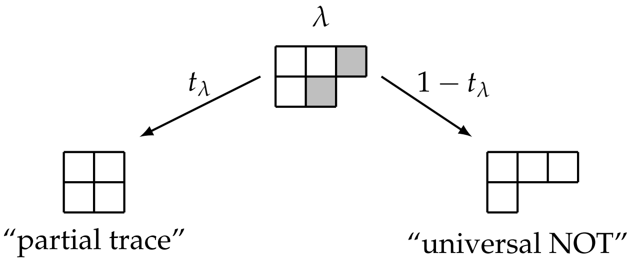
For each $\lambda \vdash n$, only two *extremal* covariant channels from $\mathbb{C}^{m_\lambda} \to \mathbb{C}^2$:



- A "dual" Clebsch–Gordan transform
- Symmetric subspaces on ℓ vs $\ell + 1$ qubits

Extremal covariant channels

For each $\lambda \vdash n$, only two *extremal* covariant channels from $\mathbb{C}^{m_\lambda} \to \mathbb{C}^2$:



- A "dual" Clebsch–Gordan transform
- Symmetric subspaces on ℓ vs $\ell + 1$ qubits
- $O(\ell \log \ell)$ gates

Main result

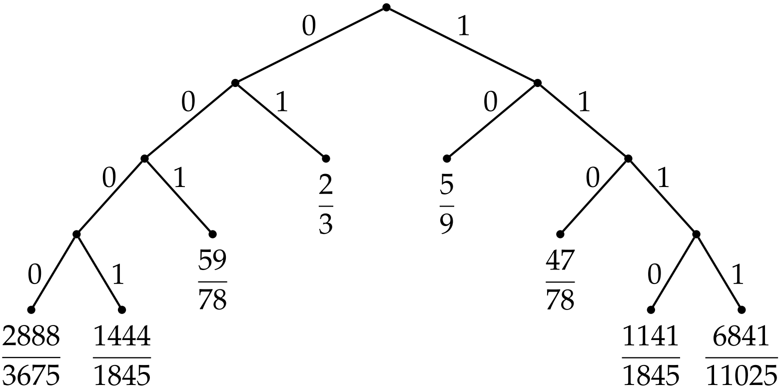
Theorem

For any symmetric and covariant n-bit boolean function

- the optimal parameters t_λ and the resulting fidelity can be determined by a linear program of size $n/2$
- optimal algorithm with $O(n^4 \log n)$ gates

Fidelities of all 7-argument functions

$\lvert x \rvert$	0	1	2	3	4	5	6	7
$f(x)$	0	1	0	0	1	1	0	1



Fidelity depends only on the gap around $n/2$ in the truth table

Open problems

- Continuous output instead of $|\psi\rangle$ vs $|\psi^{\perp}\rangle$

Open problems

- Continuous output instead of $|\psi\rangle$ vs $|\psi^{\perp}\rangle$
- Extending to qudits or to multiple outputs

Open problems

- Continuous output instead of $|\psi\rangle$ vs $|\psi^{\perp}\rangle$
- Extending to qudits or to multiple outputs
- Extending to non-symmetric and partial functions

Open problems

- Continuous output instead of $|\psi\rangle$ vs $|\psi^{\perp}\rangle$
- Extending to qudits or to multiple outputs
- Extending to non-symmetric and partial functions
- Connections with regular quantum query complexity

Open problems

- Continuous output instead of $|\psi\rangle$ vs $|\psi^\perp\rangle$
- Extending to qudits or to multiple outputs
- Extending to non-symmetric and partial functions
- Connections with regular quantum query complexity
- Applications!

Thank you!